

Juan Miguel Cano

Rodolfo Gonzalez

# Splunk Dashboard Query and Alert

(Match to color is key to understanding the description of the query)

## ATTACK MAP (Mock Map)

```
| makeresults  
  
| eval Country="United States", Count=100  
  
| append [ | makeresults  
  
| eval Country="Iran", Count=15 ]  
  
| append [ | makeresults  
  
| eval Country="North Korea", Count=75 ]  
  
| append [ | makeresults  
  
| eval Country="Russia", Count=50 ]  
  
| append [ | makeresults  
  
| eval Country="China", Count=25 ]  
  
| geom geo_countries featureIdField="Country" countfield="Count"
```

## PRIME TIME DEFENSE PIE CHART

ALL PROCESSES



## PRIME TIME DEFENSE LINE CHART

REAL-TIME OF ALL PROCESSES



## ATTACK DETECTED / SOURCE TYPE / EVENT COUNT

REAL-TIME

index="main"

(host="RISK-ANALYST1" OR host="ACCOUNTING1" OR host="ACCOUNTING2" OR  
host="CFO-LAPTOP" OR host="ip-10-0-0-175" OR host="linsecurity")

(sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" OR  
sourcetype="WinEventLog:Security" OR sourcetype="linux\_secure" OR  
sourcetype="apache\_error")

AND (

(

sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" AND

"Process Create" AND

```
(CommandLine="*powershell.exe*" OR CommandLine="*cmd.exe /c*")
)

OR

(
sourcetype="WinEventLog:Security" AND
(EventCode=4625 OR EventCode=4740)
)

OR

(
sourcetype="linux_secure" AND
"Failed password" AND
NOT user="known_good_user"
)

OR

(
sourcetype="apache_error" AND
(
"client denied by server configuration" OR
"File does not exist" OR
"script not found or unable to stat"
)
)
)

| eval AttackDetected=if(
```

```
match(_raw, "Process Create|EventCode=4625|EventCode=4740|Failed password|client
denied by server configuration|File does not exist|script not found or unable to stat"),
```

```
"Yes",
```

```
"No"
```

```
)
```

```
| stats count as EventCount by host, AttackDetected, sourcetype
```

```
| sort - EventCount
```

**This query was used as an alert and dashboard to monitor incoming attacks, source type, and event count.**

It filters events based on certain conditions related to different source types:

1. For **Sysmon Operational logs** on Windows hosts (EventCode 1- Process Create), it looks for processes created with PowerShell or cmd.exe.
2. For **Security logs** on Windows hosts (EventCode 4625 or 4740), it looks for failed login attempts.
3. For **Linux secure logs**, it looks for failed password attempts from users other than "known\_good\_user."
4. For **Apache error logs**, it looks for specific error messages indicating denied access or missing files.

After filtering, it **evaluates if an attack is detected** based on the presence of specific keywords in the raw event data and assigns "Yes" or "No" to the "AttackDetected" field.

Finally, it **calculates the count of events** grouped by host, AttackDetected, and sourcetype, sorting the results by **EventCount** in descending order.

This query helps to identify potential security incidents or anomalies across **different types of logs and hosts**.

## Alerts

## A total comprehensive Alert (too large for Dashboard Visualization)

```
(index="main" (host="RISK-ANALYST1" OR host="ACCOUNTING1" OR  
host="ACCOUNTING2" OR host="CFO-LAPTOP" OR host="ip-10-0-0-175"))
```

```
AND
```

```
(  
  
  (sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" AND ("Process  
Create" AND (CommandLine="*powershell.exe" OR CommandLine="*cmd.exe /c*")))  
OR
```

```
  (sourcetype="WinEventLog:Security" AND (EventCode=4625 OR EventCode=4740))  
OR
```

```
  (sourcetype="linux_secure" AND "Failed password" AND NOT  
user="known_good_user") OR
```

```
  (sourcetype="apache_error" AND ("client denied by server configuration" OR  
"File does not exist" OR "script not found or unable to stat"))  
))
```

```
| eval AttackDetected=if(match(_raw, "Process  
Create|EventCode=4625|EventCode=4740|Failed password|client denied by server  
configuration|File does not exist|script not found or unable to stat"), "Yes", "No")
```

```
| table _time, host, AttackDetected, sourcetype, _raw
```

```
| sort - _time
```

This query is for use with Splunk, log management, or SIEM (Security Information and Event Management) systems. It is designed to filter and analyze security-related events from various sources within our AWS Network environment.

1. **Index Specification:** It searches within the “main” index for logs coming from a set of specific hosts (‘RISK-ANALYST1’, ‘ACCOUNTING1’, ‘ACCOUNTING2’, ‘CFO-LAPTOP’, and ‘ip-10.0.0.175’). This narrows the search to logs generated by these critical or sensitive systems.

2. **Source and Event Filtering:**

- Filters for logs from the Windows Sysmon Operational log with events related to process creation ( ' "Process Create" ') that involve either PowerShell ('powershell.exe') or Command Prompt ('cmd.exe /c'). This is typically used to identify potentially malicious script executions.
- Includes Security logs from Windows with Event Codes 4625 (failed logon attempts) and 4740 (account lockout), indicating possible brute-force attacks or account compromise attempts.
- Search for failed login attempts ( ' "Failed password" ') in Linux secure logs, excluding ones from a 'known\_good\_user', helping to identify unauthorized access attempts.
- Looks for specific Apache server error messages indicating access control issues or attempts to access non-existent resources or scripts, which might suggest probing or attack attempts.

3. **Attack Detection Logic:** It uses an 'eval' command to add a field named 'AttackDetected', which flags each event as "Yes" if it matches any of the criteria described above, indicative of potential security incidents.

#### 4. Output Formatting:

- The 'table' command structures the output into a table format, showing the time of the event ('\_time'), the host from which the log originated, whether an attack was detected ('AttackDetected'), the type of log source('sourcetype'), and the raw log entry ('\_raw').
- It sorts the results in descending order by time ('- \_time'), showing the most recent events first.

This query is a powerful tool for a security analyst to quickly identify potential security incidents across different systems and log types by highlighting critical events that may indicate attack attempts or system compromises.

I went to the 10.0.0.175 and searched the logs pertaining to failed logged-in attempts with following commands and this is the first part..

I tried to check the logs in Bob's computer but he does not have the credential to do so.

**sudo cat /var/log/auth.log | grep "authentication failure"**

```
ubuntu@ip-10-0-0-175: ~$ sudo cat /var/log/auth.log | grep "authentication failure"
Mar 11 22:35:17 ip-10-0-0-175 sshd[19940]: pam_unix(sshd:auth): check pass; user unknown
Mar 11 22:35:17 ip-10-0-0-175 sshd[19940]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.0.176
Mar 11 22:35:17 ip-10-0-0-175 sshd[19915]: Connection closed by invalid user test 10.0.0.176 port 54956 [preauth]
Mar 11 22:35:17 ip-10-0-0-175 sshd[19927]: Connection closed by invalid user netadmin 10.0.0.176 port 55026 [preauth]
Mar 11 22:35:17 ip-10-0-0-175 sshd[19913]: Connection closed by invalid user web 10.0.0.176 port 54942 [preauth]
Mar 11 22:35:17 ip-10-0-0-175 sshd[19943]: Invalid user webadmin from 10.0.0.176 port 55132
Mar 11 22:35:17 ip-10-0-0-175 sshd[19943]: pam_unix(sshd:auth): check pass; user unknown
Mar 11 22:35:17 ip-10-0-0-175 sshd[19943]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.0.176
Mar 11 22:35:18 ip-10-0-0-175 sshd[19945]: Invalid user sysadmin from 10.0.0.176 port 55144
Mar 11 22:35:18 ip-10-0-0-175 sshd[19945]: pam_unix(sshd:auth): check pass; user unknown
Mar 11 22:35:18 ip-10-0-0-175 sshd[19945]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.0.176
Mar 11 22:35:18 ip-10-0-0-175 sshd[19929]: Failed password for invalid user guest from 10.0.0.176 port 55036 ssh2
Mar 11 22:35:18 ip-10-0-0-175 sshd[19921]: Connection closed by invalid user administrator 10.0.0.176 port 54980 [preauth]
Mar 11 22:35:18 ip-10-0-0-175 sshd[19947]: Invalid user netadmin from 10.0.0.176 port 55154
Mar 11 22:35:18 ip-10-0-0-175 sshd[19947]: pam_unix(sshd:auth): check pass; user unknown
Mar 11 22:35:18 ip-10-0-0-175 sshd[19947]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.0.176
Mar 11 22:35:18 ip-10-0-0-175 sshd[19949]: Invalid user guest from 10.0.0.176 port 55168
Mar 11 22:35:18 ip-10-0-0-175 sshd[19949]: pam_unix(sshd:auth): check pass; user unknown
Mar 11 22:35:18 ip-10-0-0-175 sshd[19949]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.0.176
Mar 11 22:35:18 ip-10-0-0-175 sshd[19951]: Invalid user user from 10.0.0.176 port 55170
Mar 11 22:35:18 ip-10-0-0-175 sshd[19951]: pam_unix(sshd:auth): check pass; user unknown
Mar 11 22:35:18 ip-10-0-0-175 sshd[19951]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.0.176
Mar 11 22:35:18 ip-10-0-0-175 sshd[19954]: Invalid user web from 10.0.0.176 port 55190
Mar 11 22:35:18 ip-10-0-0-175 sshd[19953]: Invalid user test from 10.0.0.176 port 55174
Mar 11 22:35:18 ip-10-0-0-175 sshd[19953]: pam_unix(sshd:auth): check pass; user unknown
Mar 11 22:35:18 ip-10-0-0-175 sshd[19953]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.0.176
Mar 11 22:35:18 ip-10-0-0-175 sshd[19954]: pam_unix(sshd:auth): check pass; user unknown
Mar 11 22:35:18 ip-10-0-0-175 sshd[19954]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.0.176
Mar 11 22:35:18 ip-10-0-0-175 sshd[19932]: Failed password for invalid user web from 10.0.0.176 port 55062 ssh2
Mar 11 22:35:18 ip-10-0-0-175 sshd[19931]: Failed password for invalid user user from 10.0.0.176 port 55048 ssh2
Mar 11 22:35:18 ip-10-0-0-175 sshd[19957]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.0.176 us
er=root
```

```
Mar 11 22:35:28 ip-10-0-0-175 sshd[20039]: Invalid user admin from 10.0.0.176 port 57754
Mar 11 22:35:28 ip-10-0-0-175 sshd[20031]: Failed password for invalid user user from 10.0.0.176 port 57670 ssh2
Mar 11 22:35:28 ip-10-0-0-175 sshd[20039]: pam_unix(sshd:auth): check pass; user unknown
Mar 11 22:35:28 ip-10-0-0-175 sshd[20039]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.0.176
Mar 11 22:35:28 ip-10-0-0-175 sshd[20001]: Connection closed by invalid user administrator 10.0.0.176 port 57440 [preauth]
Mar 11 22:35:28 ip-10-0-0-175 sshd[20041]: Invalid user administrator from 10.0.0.176 port 57756
Mar 11 22:35:28 ip-10-0-0-175 sshd[20041]: pam_unix(sshd:auth): check pass; user unknown
Mar 11 22:35:28 ip-10-0-0-175 sshd[20041]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.0.176
Mar 11 22:35:28 ip-10-0-0-175 sshd[20033]: Failed password for invalid user web from 10.0.0.176 port 57684 ssh2
Mar 11 22:35:28 ip-10-0-0-175 sshd[20016]: Connection closed by invalid user admin 10.0.0.176 port 57562 [preauth]
Mar 11 22:35:28 ip-10-0-0-175 sshd[20011]: Connection closed by invalid user user 10.0.0.176 port 57530 [preauth]
Mar 11 22:35:28 ip-10-0-0-175 sshd[20033]: Connection closed by invalid user web 10.0.0.176 port 57684 [preauth]
Mar 11 22:35:28 ip-10-0-0-175 sshd[20043]: Invalid user webadmin from 10.0.0.176 port 57778
Mar 11 22:35:28 ip-10-0-0-175 sshd[20043]: pam_unix(sshd:auth): check pass; user unknown
Mar 11 22:35:28 ip-10-0-0-175 sshd[20043]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.0.176
Mar 11 22:35:28 ip-10-0-0-175 sshd[20044]: Invalid user sysadmin from 10.0.0.176 port 57780
Mar 11 22:35:28 ip-10-0-0-175 sshd[20044]: pam_unix(sshd:auth): check pass; user unknown
```

Now I check when they actually get in with the following command:

`sudo cat /var/log/auth.log | grep "sshd.*Accepted"`

```
Mar 12 23:26:58 ip-10-0-0-175 sshd[26957]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.0.126 user=ubuntu
Mar 12 23:27:55 ip-10-0-0-175 sshd[26961]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.0.176
Mar 12 23:28:28 ip-10-0-0-175 sshd[26961]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.0.176
ubuntu@ip-10-0-0-175:~$ sudo cat /var/log/auth.log | grep "sshd.*Accepted"
Mar 10 04:09:24 ip-10-0-0-175 sshd[7885]: Accepted password for ubuntu from 10.0.0.176 port 49398 ssh2
Mar 11 06:55:33 ip-10-0-0-175 sshd[13583]: Accepted password for ubuntu from 10.0.0.176 port 50203 ssh2
Mar 11 07:39:03 ip-10-0-0-175 sshd[13821]: Accepted password for ubuntu from 10.0.0.176 port 50699 ssh2
Mar 11 16:40:52 ip-10-0-0-175 sshd[15780]: Accepted password for ubuntu from 10.0.0.176 port 51620 ssh2
Mar 12 23:28:36 ip-10-0-0-175 sshd[26964]: Accepted password for ubuntu from 10.0.0.176 port 59446 ssh2
ubuntu@ip-10-0-0-175:~$
```

Here you can see that 10.0.0.126 is also attempting to ssh.

<https://docs.google.com/presentation/d/1zaCPbFnbqMlyAIHtUVqfTDB549ltnrttLIhiqUStbrg/edit?usp=sharing>